

## The complaint

Mr P complains that HSBC UK Bank plc ('HSBC') hasn't reimbursed the funds he lost when he fell victim to a scam.

## What happened

Mr P has brought a complaint through a professional representative.

### *What Mr P says*

Mr P says that he was introduced to an investment opportunity with a company I'll to as H in this decision by a good friend of his. The first two payments he made in respect of the investment were to a team leader at H (D in the table below) to introduce Mr P and two family members. These deposits were then reflected as tokens on an exchange. Subsequent transactions were made to Mr P's own cryptocurrency account and were passed via an exchange to H's platform. Mr P continued to invest as it appeared from online meetings that others were making profits.

Mr P recognised he was the victim of a scam when H didn't pay out any funds and the platform froze his funds meaning he was unable to withdraw them. He then researched ways of recovering his funds and came across a company I'll refer to as S. After sending an enquiry email Mr P exchanged messages with an agent of S who was confident Mr P's funds could be recovered. Mr P was asked to open a cryptocurrency account and was told £500,900.76 had been returned to this account. When the funds didn't credit the account, Mr P was told that it was a known issue, and that trading was a way to resolve it. The payments Mr P made in October 2022 related to the recovery of his funds.

I have set out in the table below the scam transactions Mr P made.

Transaction	Date	Amount	Payee
1	21/10/21	£3,750	Individual - D
2	02/11/21	£870	Individual - D
3	28/02/22	\$10,060 + fee	Crypto exchange
4	11/03/22	\$7,560 + fee	Crypto exchange
5	28/03/22	\$3,575 + fee	Crypto exchange
6	27/04/22	\$12,060 + fee	Crypto exchange
7	12/05/22	\$11,273.18 + fee	Crypto exchange
8	16/05/22	\$3,760 + fee	Crypto exchange
9	13/06/22	\$13,060 + fee	Crypto exchange
10	09/08/22	\$1,261.75 + fee	Crypto exchange
11	11/10/22	\$38,550 + fee	Crypto exchange

12	11/10/22	\$15,650 + fee	Crypto exchange
13	14/11/22	\$20,050 + fee	Crypto exchange

Mr P didn't recover any funds through S and recognised he was the victim of a further scam. His representative sent a letter of complaint to HSBC in September 2023.

HSBC didn't agree to reimburse Mr P. In respect of the first two transactions HSBC considered its liability under the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code). It said it provided an effective warning and that had Mr P followed the advice given the scam would have been uncovered. HSBC also said it had done what it could to recover Mr P's funds.

The remaining transactions were to an account in Mr P's own name at a cryptocurrency exchange. HSBC said that as funds were lost from this account rather than Mr P's HSBC account, it wasn't liable.

Mr P was unhappy with HSBC's response and brought a complaint to this service.

#### *Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. For the two transactions covered by the CRM Code, the investigator said HSBC could fairly rely on an exception to reimbursement and that it had tried to recover Mr P's funds. The investigator said that all the other transactions (to a cryptocurrency exchange), weren't sufficiently unusual or out of character given the previous operation of the account that HSBC ought to have intervened. This was because Mr P had made similar high value payments before the scam.

Mr P didn't agree with the investigator's finding and asked for a decision, so his complaint was passed to me. He said the transactions were unusual and HSBC had a responsibility to protect him from fraud and to provide appropriate warnings. In particular, Mr P referred to BSI PAS 17271 and said HSBC should have had concerns for a number of reasons including the high frequency of the payments, the significant amount transferred in a short timescale and the high values (in particular the near \$40,000 transaction).

After reviewing Mr P's complaint, I thought HSBC should reimburse transactions one and two, so I issued a provisional decision on 18 September 2024. In the "What I've provisionally decided – and why" section of my provisional decision I said:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position in law is that HSBC is expected to process payments that a customer authorises it to make, in accordance with the terms and conditions of the customer's account and the Payment Services Regulations (PSR's). And banks generally have a contractual duty to make payments in compliance with the customer's instructions.

#### *Transactions 1 and 2*

These payments were made to an individual who was clearly connected to H (as Mr P has provided evidence of his communications with D relating to his investment with H) and are covered by the CRM Code.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:

- The customer made payments without having a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate

There are further exceptions outlined in the CRM Code that do not apply to this case.

I'm satisfied Mr P had a reasonable basis for believing the investment opportunity offered by H was genuine. It was introduced to him by an old friend who he trusted. This friend explained to Mr P that his questions had been answered in a video call. It's also clear from the emails and messages Mr P exchanged with this friend that he received multiple links to information about how H operated, compliance information, testimonials, training material and videos. There was also a lengthy due diligence document which contained links to articles and videos. I think all these factors would be persuasive to an inexperienced investor. Mr P says he completed research and reviews were mixed, as can often be the case.

Mr P's CRM Code caught payments were going to a manager he had communicated with, and his friend had previously paid. In the circumstances, I don't consider Mr P acted unreasonably in paying the same person.

I appreciate that HSBC provided Mr P with a general investment warning. Whilst the warning contains some relevant information, there's no mention at all of cryptocurrency so it lacked impact, and I can see why it didn't resonate with Mr P or lead him to take additional steps. So I'm not persuaded the warning HSBC provided to Mr P negatively impacts his reasonable basis for belief.

So, under the CRM Code, Mr P should receive a full refund of transactions one and two.

### *Transactions 3 to 13*

These transactions aren't covered by the CRM Code as they were made to an account held in Mr P's name.

Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment.
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-

stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

I've carefully considered the activity on Mr P's accounts (GBP and USD) to decide if HSBC acted reasonably in processing Mr P's payment requests. Having done so, I'm satisfied that HSBC acted reasonably in processing all the remaining transactions in the table above without intervening.

I say this because they were in line with previous account activity. For example, on 21 September 2021 Mr P made a payment of \$15,570 to an international money transfer service. On 11 January 2022 Mr P made two payments (\$15,570 and \$2,750) to the same service. A week later he made a further payment of \$13,750 and in August 2022 he made a payment of \$50,016. This transaction is similar in value to the two transactions on 11 October 2022 added together. Mr P also made high value payments from his GBP account.

In the circumstances, I'm not persuaded HSBC ought reasonably to have taken additional steps before processing Mr P's payment requests, particularly as they were spread over a period from February to October 2022, and the value of the transactions fluctuated. I don't consider these transactions matched common scam types.

In its letter of complaint Mr P's representative has included a loss of £20,050 on 14 October 2022 and said that Mr P lost £18,820 of this amount. I can't see this figure on any of Mr P's statements. I have also asked HSBC about it, but HSBC is unable to identify the transaction. So I can't consider this transaction. In any event, I'm uncertain how Mr P can have lost only part of this amount.

Overall, I'm provisionally minded to require HSBC to refund transactions one and two, plus interest as set out below.

#### *Responses to my provisional decision*

Mr P didn't agree with my provisional findings. He provided evidence of a \$20,050 transaction on 14 November 2022 (not October as previously stated) and made the following points:

- The transactions he made were highly unusual and should have flagged on HSBC's fraud prevention systems. Only one of the transactions I referred to pre-dated investments Mr P made with fraudsters.
- There is a key difference between previous transactions and those in the table above as Mr P was paying cryptocurrency exchanges. Mr P had never previously invested in cryptocurrency and HSBC should have flagged the payments as a result.
- It is good industry practice that payments over £5,000 to a new payee are flagged for further intervention.
- HSBC didn't intervene at all so Mr P was unable to take necessary precautions to protect himself.
- Had the bank intervened and asked appropriate questions the scam would have been uncovered.
- At the time of the scam transactions Mr P was vulnerable. He was responsible for caring for his mother who was extremely ill and was subsequently diagnosed with cancer.
- Through the course of these transactions Mr P fell victim to two investment scams and a recovery scam. If HSBC had intervened appropriately the recovery scam could have been completely avoided.

HSBC also disagreed with my provisional decision. It referred to previous points made and added:

- Even if HSBC had questioned Mr P about the investment opportunity it is unlikely it would have deterred him from continuing or convinced him to make checks. This is because Mr P was introduced to H by a friend who was already investing and had seen documentation about the investment. And although Mr P said he had completed checks which were positive, this service has seen mixed reviews. This suggests Mr P hadn't properly looked at reviews.
- HSBC provided a warning which advised Mr P to check that the company was FCA authorised. If Mr P had done this, he'd have seen a warning issued by the FCA in March 2021 stating that H wasn't authorised. The warning also advised Mr P to thoroughly research the company.
- Mr P didn't receive any documentation prior to investing – which is unusual.

### **What I've decided – and why**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having carefully considered the responses I have received from both parties my final decision is the same as my provisional decision, and for the same reasons.

I have included the £20,500 transaction in the above table of loss as Mr P has now provided evidence that the transaction was made on 14 November 2022 (not October as previously stated). This transaction was from Mr P's GBP account.

Neither party has suggested that HSBC can fairly rely on the reasonable basis for belief exception, so I won't comment further on the two CRM caught transactions.

I turn to the remaining payments not covered by the CRM Code. To determine whether a transaction is so unusual and out of character that a bank ought reasonably to have concerns there may be a risk of fraud and intervene I need to consider account activity as well as other information available to HSBC at the time. This 'trigger' point will be different depending on what is normal activity for that particular customer.

When the scam payments started there was nothing unusual about them and they were very much in line with multiple payments from Mr P's accounts. Mr P says payment three should have triggered HSBC's fraud detection systems, but I disagree. In September 2021 Mr P made a higher value payment (\$15,570) so I don't consider payment three stood out. Whilst it was to a cryptocurrency exchange, I'm mindful that many such payments are legitimate. Then by the time Mr P made payments of \$12,060 and \$11,273 he had also made a £20,250 transaction from his GBP account. And the more significant payments made by Mr P during the recovery scam followed a payment of \$50,016 in August 2022 as well as other high value payments.

I've taken into account that these payments were made to a cryptocurrency provider and I'm aware that scams involving cryptocurrency are becoming increasingly prevalent and well known to banks. But, at the time these payments were made, I think it was reasonable for the bank to take into account a range of factors when deciding whether to make further enquiries of its customer about a particular payment. The transactions in this case are spread out over a period of over a year and are not in quick succession.

I'm really sorry to hear that Mr H was vulnerable when the payments were made. Under the CRM Code a customer is entitled to full reimbursement if they were unable to protect themselves from the scam they fell victim to. But I have already said Mr P should be fully reimbursed under the CRM Code. In respect of the other payments, I can't see that HSBC was made aware of any vulnerability or was asked to provide any additional support to Mr P.

Overall, whilst I'm very sorry to hear about Mr P's loss and personal circumstances, I can only fairly ask HSBC to reimburse the loss that is covered by the CRM Code.

**My final decision**

For the reasons given, I to require HSBC to:

- Pay Mr P £4,620; and
- Pay interest on the above amount at the rate of 8% simple per year from the date HSBC made its decision not to reimburse until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 13 November 2024.

Jay Hadfield  
**Ombudsman**